Social Networks and Electronic Discovery

by Daniel B. Garrie, Anna S. Park and Yoav M. Griver

When a lawyer seeks evidence in civil or criminal litigation, his or her remit is to seek evidence wherever it exists. Today, that evidence often exists on social networking sites and other digital locations. Consider the following hypothetical:

An employee working in a pharmaceutical company as a drug sales representative goes on maternity leave, and a new manager takes over. The new manager sexually harasses the employee with verbal remarks; inappropriate emails sent from his home and work computers; lewd Facebook messages sent via his work computer; posts of inappropriate pictures he obtained from the employee's public Facebook account on the company's intranet; and countless messages sent via his iPhone, which he uses personally and for work. Not surprisingly, the employee files a harassment complaint with the company's management. Management circulates emails discussing the harassment complaint and reports it to its human resources department (HR). In accordance with company policy, HR logs the complaint in the company-hosted corporate PeopleSoft platform. HR has dialog with management about the appropriate course of action, but no action is taken. The employee quits, and several of the managers post on their Facebook accounts that they were upset about the employee leaving. It is anticipated the employee will file a lawsuit.

The hypothetical demonstrates the complexity that often ensues given the convergence of social networks, intranets, email, and cloud-based HR systems in today's modern workplace.

This article does not (and cannot) address every issue dealing with the discovery of social networking sites, but will examine basic issues arising from social networking and legal discovery that should be considered by every practitioner.

Discoverability of Social Networking Sites

Only a few jurisdictions have ruled on whether one should have a reasonable expectation of privacy in information posted on the Internet through various social networking sites. The general consensus among these courts is that one may not have an expectation of privacy in connection with such postings.[1]

With regard to the discoverability of information posted on social networking sites, in general courts have engaged in the following three-part analysis: 1) does the user of social networking sites have a reasonable expectation of privacy of information that is posted on the sites; 2) under the state's discovery rules is the information sought on the social networking sites relevant to the litigation; and 3) is the request based on a factual predicate that an examination of the non-public portions of the social networking site would lead to relevant information.

User's Privacy Rights

Courts have generally held that a user has no reasonable expectation of privacy on information the user posts on social networking sites.[2]

In *McMillen v. Hummingbird Speedway, Inc.*,[3] the Court of Common Pleas for Jefferson County, Pennsylvania, granted the defendants' motion to compel discovery of the plaintiff's Facebook and MySpace accounts in connection with the plaintiff's claim of damages for injuries he allegedly sustained during a stock car race. The court held the plaintiff did not enjoy a reasonable expectation of privacy of information posted on his Facebook and MySpace accounts because: 1) Facebook's own privacy policy cautions that contents shared by the user may be disclosed to the public at large, regardless of whether the user sets a privacy setting that includes only his or her friends, and that even after content is removed

from the user's account the information may remain viewable elsewhere; 2) Facebook advises users that Facebook operators may disclose information in response to subpoenas, court orders or other civil or criminal requests if it has a good faith belief compliance is required by law; and 3) both Facebook and MySpace operators have unfettered access to each users' profile, content and postings and may, at their option, choose to review, post or remove any content posted by the user.[4]

In *Largent v. Reed*,[5] the Court of Common Pleas for Franklin County, Pennsylvania, refined the holding in *McMillen,* stating that by definition a social networking site's sole purpose is to promote the sharing of information with other users and the public at large. Therefore, there can be no reasonable expectation of privacy, given that nearly all information posted on a social networking site such as Facebook is shared with third parties.[6]

Likewise, in *Romano v. Steelcase Inc.*,[7] the Suffolk County Supreme Court for the state of New York granted the defendant's motion by order to show cause for access to plaintiff Kathleen Romano's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information in connection with her claims for damages related to personal injuries she allegedly suffered. The Court held that users of social networking sites do not have a "legitimate expectation of privacy in materials intended for publication or public posting."[8] Citing to holdings by the Second Circuit[9] and the United States District Court of New Jersey,[10] where the federal courts have held that one loses his or her expectation of privacy in Internet postings and emails that have reached their recipients, the user of social networking sites such as Facebook and MySpace may not have an expectation of privacy on entries they post on these sites.[11] The Court further recognized that both Facebook and MySpace does not guarantee privacy and, in fact, expressly advise their respective users that sharing of information is done at the user's own risk.[12]

Relevancy to the Issue in Dispute

As set forth above, privacy has not proven to be an obstacle to discovery of material posted on social networking sites. However, like traditional discovery, parties must still demonstrate the information they seek on the social networking sites or their request for access to social networking sites is relevant to the issues in dispute. This relevancy analysis varies depending on the jurisdiction. For example, in Pennsylvania discovery rules are very broad and liberal with a limited number of privileges; nearly any material is discoverable as long as there is some relevance to the issue in dispute.[13] Florida also employs broad discovery rules where as long as discovery is relevant to the subject matter of the case and admissible or reasonably calculated to lead to admissible evidence, it is allowed.[14] Although arguably not as broad, New York's discovery rules still provide for full disclosure of all non-privileged information "material and necessary" to the defense or prosecution of an action.[15]

Most jurisdictions favor liberal discovery, regardless of the admissibility of evidence, in order to allow the parties full opportunity to gather information that may be helpful and/or useful in the prosecution or the defense of an action. In federal court, the discovery rules are governed by the Federal Rules of Civil Procedure, which also favor broad discovery of all non-privileged relevant evidence.[16]

In *Largent*,[17] the court held that photographs and texts posted on the publicly available portion of the plaintiff's Facebook page showing the plaintiff enjoying her life with her family and going to the gym contradicted her claims of serious and severe physical injuries she allegedly suffered as a result of a motor vehicle accident involving the defendant. Accordingly, the posted material was relevant to the issue of damages, and therefore was discoverable.

Similarly, in *Simms v. Lewis*,[18] the Court of Common Pleas of Indiana County, Pennsylvania, granted the defendant's motion to compel production of plaintiff Brittni Simms's social networking information based on a showing the plaintiff had posted on the public front page of her myYearbook account a statement: "Chillin with my girl tonight. were gonna do some Zumba Fitness :) so excited!!! HTC :p."[19] The court held that where Simms had averred that, as a result of injuries she sustained following a collision with the defendant's vehicle, she was deprived of the ordinary pleasures of life, her statement in reference to attending a fitness class was sufficient to establish that additional relevant information may exist on the non-public portion of her account. The court then ordered the defendant be granted access to the non-public areas of the myYearbook account.[20]

However, in both *Mailhoit v. Home Depot U.S.A., Inc.*[21] and *Tompkins v. Detroit Metropolitan Airport*,[22] courts have denied the defendants' respective motions to compel discovery of the plaintiffs' social networking sites, holding the information sought on the sites was not reasonably calculated to lead to the discovery of admissible evidence.

Factual Predicate Must Be Demonstrated

Irrespective of the foregoing, a court may deny access to information contained in social networking sites based on whether the party seeking access has demonstrated a factual predicate that additional discovery of the site would lead to relevant information. For example, courts have generally granted access to a defendant in a personal injury litigation where damages are an issue,

based on photographs or textual posts the defendant was able to procure on the publicly available portion of the complaining plaintiff's Facebook or other social networking site and present to the court in support of the defendant's request for access. Without such preliminary showing, courts have been reluctant to grant access and disfavor attempts that may look like mere fishing expeditions.

Indeed, the *Largent* court cautioned the court's holding should not be construed as a "carte blanche entitlement" to access a party's Facebook and MySpace accounts in any and all personal injury cases where damages are an issue.[23] It held that, as with all discovery, "fishing expeditions" are not permitted and the party seeking access to any social networking sites must demonstrate a good-faith basis for seeking such discovery. To establish a good-faith basis, the party must demonstrate to the court, through establishment of a factual predicate (*e.g.*, photographs, textual posts, status updates) found through an initial search of public sites, that discovery of the social networking site is reasonably calculated to lead to the discovery of admissible evidence.[24]

Likewise, in *Caraballo v. City of New York*[25] the Richmond County Supreme Court for the state of New York denied defendant Campa Construction Corp.'s motion to compel discovery of plaintiff Pedro Caraballo's "current and historical Facebook, MySpace and Twitter pages and accounts, including all deleted pages and related information," holding Campa's discovery demands were overly broad and failed to establish a factual predicate with respect to what relevant information the sites may contain. Likewise, in *Progressive Ins. Co. v. Herschberg*[26] the Queens County Supreme Court of the state of New York denied the insurer's request for "unlimited access" to the plaintiff insured's Facebook pages, holding the insurer's request was overly broad and there was no showing that "the material sought was necessary and not cumulative."

Applying ESI Discovery Standards to Social Networking Sites

As potentially discoverable electronic information, contents posted on social networking sites may be governed by the same principles that govern electronically stored information (ESI). Although the authors are currently unaware of any courts that have definitively held as such, it is believed this will be the logical next step. Therefore, the following will discuss key concepts that may arise in the context of discovery of electronic data published and maintained on social networking sites (SNS) applying the rules and procedure utilized in electronic discovery of ESI, as well as issues that may arise of which practitioners should be aware.

In general, electronic discovery of ESI involves the following steps: 1) identification; 2) preservation; 3) collection; 4) analysis; 5) processing; 6) review; and 7) production. Given this article's narrow topic of discoverability of SNS, the focus of this discussion will be on the first three steps: identification, preservation and collection.

Identification and Preservation

Like all discovery, once litigation is reasonably anticipated, counsel should have a full and in-depth discussion with their client to identify all sources of SNS accessed by the client during the time period relevant to the anticipated litigation, as well as sites where content involving the client may be posted. SNS accessed by the client may include the client's personal Facebook, MySpace and Google+ sites, to name just a few.[27] However, it is also important to identify content that may be posted on sites to which the client does not have access. For example, although the user of a Facebook page may not directly post a photo or text on the user's own page, any one of the user's friends will be able to 'tag' the user on their own Facebook page. These photos and text would be governed by the friend's privacy settings, and potentially be available to the public without the user's knowledge or authorization. Of course, the user has the right to request the friend 'untag' the user in the photo or text, but the friend may not comply, or it may simply be too late.

Based on existing legal authority, most courts require demonstration of a factual predicate that relevant information exists in the depths of the SNS the party seeks to discover. Most often, this factual predicate is obtained through a basic Internet search for the name(s) of the opposing party. If any part of the SNS content is publicly available it will be revealed during such an Internet search. Therefore, it may be useful to conduct a basic Internet search during the identification step of the discovery process, either to uncover publicly available information or to seek further discovery of the non-public portions of the adversary's SNS.

Once the sources of SNS are identified, steps must be taken to preserve the SNS data. The client will be deemed to have command, custody and control over the content posted on his or her personal SNS, and a legal hold should be placed on the SNS to preserve all content, history and data.

A legal hold (or litigation hold) is a process by which an organization preserves and protects from spoliation all forms of information and data (both paper and ESI) that may be relevant to the issues involved in litigation when litigation is reasonably anticipated or the organization receives notice of a legal dispute, whichever is earlier. A legal hold helps the organization fulfill its preservation obligations. In light of its purpose, there is no reason to exclude SNS from a legal hold.

In general, the concept of a legal hold

is most often associated with organizations that take affirmative steps to notify their custodians of data of the organization's obligation to preserve potentially relevant information in the face of notice of actual or reasonably anticipated litigation. Little should change when it comes to SNS maintained by the organization and in the organization's command, custody and control. For example, the organization's Facebook page should be treated the same as any other ESI; all content that exists at the time the litigation hold is placed must be preserved, including all history and even previously deleted data. Similarly, an individual litigant who reasonably anticipates or is on notice of litigation must also place on hold all content that exists on the litigant's SNS, including all history and deleted data.[28] In addition, it would be advisable for counsel to advise his or her client to suspend posting on all SNS and to request third parties to cease posting any photos, texts, videos or other content on the third parties' respective SNS for the duration of the litigation.

The issue may be trickier when dealing with SNS that is not in an organization's or litigant's command, custody or control. For example, in the hypothetical, would the company be obligated to place a legal hold on all SNS maintained by its employees, or just on the managers? If the company fails to place a legal hold on the information, would it be deemed to have failed in its obligation to preserve possibly relevant evidence concerning the plaintiff's sexual harassment claims? The SNS is not within the company's command, custody or control, so how would the company be able to enforce compliance with any legal hold it places and, practically speaking, on what would the company place the legal hold? Moreover, if an employee deletes data from his or her personal SNS, would the company be liable for spoliation? Should the analysis change if the employee accessed his or her personal SNS through the company's work computer?

Although factually distinguishable, a ruling by New York's Supreme Court, Appellate Division, First Department, involving the deletion of ESI through normal business operations by a non-party (New York University (NYU) Langone Medical Center) may be insightful in answering this question. In *Tener v. Cramer*,[29] the First Department reversed the trial court's decision that denied the plaintiff's motion to hold non-party NYU in contempt for failing to comply with a judicial subpoena that requested it produce the identity of all persons who accessed the Internet on April 12, 2009, the date a defamatory post originated from a computer (which the plaintiff was able to identify based on an IP address of the computer she was able to trace) in the command, custody and control of NYU.[30] In opposition to the plaintiff's motion for contempt, NYU stated that computers, such as the one identified by the plaintiff, that simply access the web through NYU's portal, appear as a text file listing that is automatically written over every 30 days. NYU further stated that it did not possess the technological capability or software to retrieve a text file created more than a year before the subpoena was served.[31]

In reviewing the principles and guidelines set forth by the Federal Rules of Civil Procedure, New York's Uniform Rules for the Trial Court, guidelines for ESI discovery published by the Commercial Division for the Supreme Court, Nassau County, as well as commentary published by the Sedona Conference, the First Department held that NYU did not offer any evidence to show it made an effort to recover the "overwritten" data, relying simply on the fact that it was a non-party, and therefore not required to install any forensic software that may be able to retrieve the lost data.[32] The Court found the plaintiff demonstrated "good cause" that her source for identifying the individual who defamed her was solely NYU; that she had no other source for this information; and that, although the data was difficult to access, it was not permanently deleted.[33] Therefore, the Court remanded the case back to the trial court to order a hearing to determine, among other things, whether the data sought by the plaintiff was indeed written over, and therefore lost, as NYU maintained, or retrievable through the use of forensic software, and a budget for the cost of retrieving the data if retrievable.[34] The Court did recognize NYU's status as a non-party and ordered that if NYU is able to produce the data, the cost of production, including the cost of disruption of NYU's normal business operations, should be allocated to the plaintiff.[35]

Extending the First Department's analysis to the present hypothetical, if the plaintiff were to subpoena the company for the names of all individuals who accessed their Facebook accounts through their work computers, the company would be required to provide the information. Moreover, it does not seem far-fetched that a court may find that if the company has knowledge its employees access their Facebook accounts through their work computers it would have an obligation to announce a legal hold on all content existing at the time of the legal hold to preserve existing data and prevent its deletion.

However, if the employee accesses his or her Facebook account through their home computer and deletes pertinent data, would the court find the company has engaged in spoliation, or it failed in its obligation to preserve possibly relevant evidence?

Superficially, it would seem in the context of SNS that is not within the company's command, custody and control the company's preservation duties should end with the announcing of a legal hold. However, the issue again is enforcement. An announcement of a legal hold without any consequences for

failure to actually preserve is like a dog with a bark but no bite. Compliance is unlikely if a company's obligation is satisfied by the mere announcement of a legal hold without further consequence, at least for the company, where the employee then fails to preserve in compliance with the hold.

Collection

Less complicated than the issue of identification and preservation is the collection and ultimate production of SNS. Collection and production of data contained in SNS is even less cumbersome than the collection and production of other ESI because the data is self-contained in each specific SNS and access is all that is required to collect and produce it. Indeed, as the *Largent* court aptly noted, allowing a litigant access to the SNS is the least burdensome way to conduct discovery.[36] Assuming the parties have agreed on the discoverability of SNS content, or a court has compelled the discovery of SNS, all that is needed is the production of the user's login and password information. The court can set a finite period of time in which the litigant has access to the SNS using the login and password, and after that time period elapses the user can change his or her password to deny further access. To the extent the litigant seeks production of deleted data, the user can provide authorization and consent the litigant can serve on the specific SNS operator to compel production of the deleted data.[37]

Conclusion

Discovery of social networking sites can, in some ways, be less complex due to the lack of privilege and privacy issues. However, it can be more complicated due to the public nature of the sites and the difficulty in locating a custodian for identification and preservation purposes. Just five years ago, discovery of ESI was the hot topic discussed at every continuing legal education program and conference. The issue of e-discovery is still a relevant and dynamic area of law. However, the introduction, publication and adoption of countless case law, guidelines, principles and rules have stabilized what once seemed an uncontainable and daunting task of identifying, preserving, collecting, analyzing, reviewing and producing intangible data. As is inevitable with the ever-evolving and growing field of technology, data posted and contained on social networking sites throws a wrinkle in a process that for the time being seems established. ⚖

Endnotes

1. *Thompson v. Autoliv ASP, Inc.*, No. 09-01375 2012 U.S. Dist. LEXIS 85143 (D. Nev. June 20, 2012) (granting defendant's motion to compel discovery of plaintiff's social networking sites but limiting relief to avoid "annoyance, embarrassment, oppression or undue burden" on plaintiff); *Davenport v. State Farm Mut. Auto. Ins. Co.*, No. 11-632, 2012 U.S. Dist. LEXIS 20944 (M.D. Fla. Feb. 21, 2012) (holding contents of social networking sites are neither privileged nor protected by any right of privacy and therefore discoverable under Rule 34 of the Federal Rules of Civil Procedure); *Offenback v. LM Bowman, Inc.*, No. 10-1789, 2011 U.S. Dist. LEXIS 66432 (M.D. Pa. June 22, 2011) (ordering personal injury plaintiff to turn over data on his Facebook page that contradicted his claim of injury in a form mutually agreeable to the parties); *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010) (allowing discovery of Facebook material between two plaintiffs who alleged emotional distress injuries in a Title VII sexual harassment case); *Beswick v. NW Med. Ctr., Inc.*, No. 07-020592, 2011 WL 7005038 (Fl. Cir. Ct. Nov. 3, 2011) (granting defendant's motion to compel plaintiff to provide defendant with executed consent and authorization to access plaintiff's Facebook records).
2. This analysis is limited to the United States; privacy and data protection rules in the United Kingdom and much of Europe are far more restrictive than the United States.
3. No. 113-2010, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Comm. Pl. Sept. 9, 2010).
4. *Id.*
5. No. 2009-1823, 2011 WL 5632688 (Pa. Comm. Pl. Nov. 8, 2011).
6. *Id.*
7. 907 N.Y.S. 2d 650 (Suffolk Cty. Sup. Ct. 2010).
8. *Id.*
9. *U.S. v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004).
10. *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, 568 F. Supp. 2d 556 (D.N.J. 2008).
11. *Largent , supra,* note 5.
12. *Id.*
13. Pa. R.C.P. 4003.1; *see also George v. Schirra*, 814 A.2d 202 (Pa. Super. 2002).
14. Fla. R. Civ. P. 1.280; *see also Allstate Ins. Comp. v. Langston*, 655 So.2d 91 (Fla. 1995).
15. N.Y. CPLR §3101; *see also Allen v. Crowell-Collier Pub Co.*, 21 N.Y.2d 403, 288 N.Y.S.2d 449 (1968).
16. Fed. R. Civ. P. 26(b)(1).
17. *McMillen, supra,* note 3.
18. No. 12-2289, 2012 WL 6755098 (Pa. Comm. Pl. Oct. 10, 2012).
19. *Id.*
20. *Ibid.*
21. 2012 U.S. Dist. LEXIS 131095 (C.D. Cal. Sept. 7, 2012).
22. 278 F.R.D. 387 (E.D. Mich. 2012).
23. *Tompkins*, *supra,* note 22 (*citing Zimmerman v. Weis Markets, Inc.*, 2011 WL 2065410 n.8 (Pa. Comm. Pl. May 19, 2011)).

24. *Id.*
25. No. 103477-2008, 2011 N.Y. Misc. LEXIS 1038 (Richmond Cty. Sup. Ct. March 4, 2011).
26. No. 000014-2010, 2011 N.Y. Misc. LEXIS 2323 (Queens Cty. Sup. Ct. March 30, 2011).
27. The list of active social networking sites is exhaustive. A list of the major social networking sites, excluding major dating sites, are available on Wikipedia at http://en.wikipedia.org/wiki/List_of_social_networking_websites.
28. In *Gatto v. United Air Lines, Inc.*, 2013 U.S. Dist. LEXIS 41909 (D.N.J. March 25, 2013), the court granted defendants' request for jury instruction to be given at trial that the jury may draw an adverse inference against plaintiff for failing to preserve his Facebook account and intentionally destroying evidence by permanently deleting the contents of his Facebook account after being notified of the content's relevance in the litigation and being ordered to preserve it and provide defendants with access to it.
29. 89 A.D.3d 75, 931 N.Y.S.2d 552 (App. Div. 1st Dept. 2011).
30. *Id.* at 76.
31. *Id.* at 77.
32. *Id.* at79-82.
33. *Id.* at 82.
34. *Ibid.*
35. *Ibid.*
36. *McMillen , supra,* note 3.
37. A subpoena served directly on a social networking site without the consent and authorization of the user may be quashed. In *Crispin v. Chrisitian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010), the court quashed defendants' subpoenas served on Facebook and several other social networking sites based on a finding that Facebook is an entity covered by the federal Stored Communications Act.

Daniel B. Garrie *has a B.A. and M.A. in computer science from Brandeis University, and a J.D. from Rutgers University. He is the senior managing partner at Law & Forensics LLC, a legal strategy consulting firm specializing in e-discovery, digital forensics, and cyber security.* ***Anna S. Park*** *is a senior associate in the New York office of Zeichner Ellman & Krause LLP, where she concentrates her practice on complex commercial litigation matters that include a variety of electronic discovery issues.* ***Yoav M. Griver*** *is a partner in Zeichner, Ellman and Krause LLP's litigation group, where he specializes in representing clients in complex commercial matters.*